REMARKS

Claim 1 has been amended to define that the means which outputs authentication data of the authentication apparatus of the present invention is based on a combination of a pulse voltage and a pulse interval of the random pulses generated by the random pulse generator. Claim 9 has been amended to define that the step of outputting authentication data of the authentication method of the present invention is based on a combination of a pulse voltage and a pulse interval of the random pulses generated by the random pulse generator. Claim 18 has been amended to define that the code to output authentication data of the computer readable memory medium storing an authentication program of the present invention is based on a combination of a pulse voltage and a pulse interval of the random pulses generated by the random pulse generator.

The amendments to claims 1, 9 and 18 are supported by the description in the specification on page 10, line 18, to page 11, line 1, in which it is described that a combination of voltage of the random pulse and a number of clock pulses (indicating a pulse interval of the random pulses) may be used, for example, pulses represented by combination values of (9, 5), (4, 3), (7, 6) and (10, 3).

Referring to the Action, claims 1-4, 8-11 and 15-19 are

rejected under 35 U.S.C. § 103(a) as being unpatentable over Shi (EP 0957220), in view of Shilton (WO 99/41834). Claims 6 and 13 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Shi in view of Shilton, and further in view of Barker (US 5,076,971).

Reconsideration of these rejections is respectfully requested in view of the amendments to claims 1, 9 and 18 and the remarks that follow.

The combination of Shi and Shilton, with or without Barker, fails to support a case of prima facie obviousness of the claims under 35 U.S.C. § 103(a).

In the Action the Office alleges that paragraph [0017] of Shi teaches using a voltage-controlled oscillator (VCO) for obtaining a spectrum-spreaded signal, which is used to generate true random code. (See, for example, page 3, lines 3-5, of the Action). The voltage used to control the VCO is thereby interpreted as a pulse voltage. Thus, according to the Office, the random code is generated by both a pulse voltage and a pulse interval.

However, since paragraph [0017] of Shi also discloses "[t]he output of B [M-sequence generator] is converted by a D/A convertor into the levels ...", the levels can be interpreted as an analog voltage, but not a pulse voltage. Accordingly, Shi does not teach

that the random code is generated using the pulse voltage, still less both a pulse voltage and a pulse interval.

Even if, for argument's sake, the voltage used to control the VCO is interpreted as a pulse voltage, Shi discloses nothing to indicate the feature set forth in the amended claims of the present application that authentication data is output based on a combination of a pulse voltage and a pulse interval of the random pulses.

Shilton teaches that alpha particles, a beta ray or a gamma ray released by the collapse of an atomic nucleus is detected, but this reference also is quite silent about the feature of the present invention that authentication data is output based on a combination of a pulse voltage and a pulse interval of the random pulses.

Barker teaches that a beta ray radiator includes ^{210}Pb, but this reference also is silent about the feature of the present invention that that authentication data is output based on a combination of a pulse voltage and a pulse interval of the random pulses.

By basing the authentication data on a combination of the pulse voltage and the pulse interval, the authentication data of the present invention can be created at a higher bit rate than is

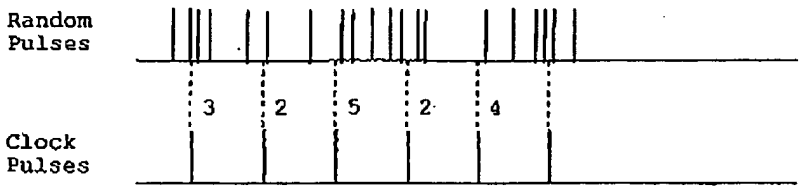
otherwise possible. This is especially an advantage in ultra-secure authentication applications involving random pulse generators based on radioactive decay where an increase of the pulse rate is not available or desirable for reasons such as radiation protection.

As a result, the present invention is neither anticipated nor rendered obvious over the cited references, whether taken singly or in combination.

Notwithstanding that the prior art Shi, Shilton and Barker references, alone or in combination, do not support the 35 U.S.C. § 103(a) rejections of the claims, an explanation of the difference in how to generate random numbers between the present invention and each of the cited references is provided below for the benefit of the Office.

Shi

According to paragraph [0015] of Shi, a "series of random numbers can be obtained by sampling said sequence of the pulses with an independent clock pulse of low frequency". That is, as shown in the following drawing, the number of pulses is counted between the clock pulses of low frequency.



In contrast, in the present invention, as shown in Fig. 9 and its description, the interval of the random pulses is measured by counting the number of clock pulses and the counted number of clock pulses can be used as a random value.

Since the random pulse generator of the present invention detects alpha particles, a beta ray or a gamma ray released by the collapse of an atomic nucleus, the present invention can obtain true random pulses. However, in Shi, an M-sequence generator (a pseudo-random generator) is used (see paragraph [0017], line 48), so that the output of the D/A convertor (i.e., the input of the VCO) also has pseudo-random characteristics (see paragraph [0017], lines 49-50). Since the VCO has linear characteristics between an input voltage and an output frequency, the output of the VCO also has pseudo-random characteristics. Subsequently, each of an output of trigger D1 and an XOR of the outputs of triggers D1 and D2 also has pseudo-random characteristics. As a result, in Shi, true

random pulses cannot be obtained.

On page 3 lines 8-9, of the Office Action, the Office alleges: "[t]he random numbers generated are determined by a sequence of pulses with random widths, thus a pulse interval" (see Shi, paragraph [0015])." However, this description is not found in paragraph [0015]. The paragraph merely states: "[a] circuit is designed to amplify and gating the noise produced by the element so as to obtain a sequence of pulses with random widths" (lines 23-25). Further, the paragraph states "[s]ince the pulse widths of said sequence of the pulses depend on the noise of the avalanche effect and various parameters of the circuit (e.g. amplifying gain, threshold value, working point, etc.) …" (lines 28-31). Accordingly, the Office's allegations are not correct.

Shilton

As seen from Claim 1 and Fig. 1 of Shilton, random numbers are created according as a random pulse is detected or not in a predetermined time period. That is, a binary number "1" is output when the count is 0 and a binary number "1" is output when the count is >0 (see page 8, lines 26-27).

In the method of Shilton, as described in lines 20-22 on page 3, "the comparisons used to generate the binary numbers are required to have a probability of exactly ½ or else the numbers

produced are not truly random", and as described in lines 27-29 on page 8, "it [this method] has the disadvantage that if the mean pulse rate is not exactly equal to ln2, the probability of outputting binary "1" is then not exactly equal to binary "0".

In contrast, in the present invention, as before-mentioned, the interval of the random pulse is measured by counting the number of clock pulses and the counted number of clock pulses can be used as a random value. Accordingly, the present invention does not have the above-mentioned disadvantages of Shilton reference.

For the above reasons, removal of the 35 U.S.C. § 103(a) rejections and a notice of allowability of the claims are believed to be in order and are respectfully requested.

The foregoing is believed to be a complete and proper response to the Office Action dated July 30, 2010.

In the event that this paper is not considered to be timely filed, applicant hereby petition for an appropriate extension of time. The fee for any such extension and any additional required fees may be charged to Deposit Account No. 111833.

Respectfully submitted,
KUBOVCIK & KUBOVCIK

Ronald J. Kubovcik
Reg. No. 25,401

Crystal Gateway 3
Suite 1105
1215 South Clark Street
Arlington, VA 22202
Tel: (703) 412-9494
Fax: (703) 412-9345
RJK/ff